AN INTEGRATED CIRCUIT CHIP MADE SECURE AGAINST THE ACTION OF ELECTROMAGNETIC RADIATION

The present invention relates to integrated circuit (IC) chips for incorporating in portable articles, in particular of card format.

IC cards are generally used in applications in which it is essential for confidential information to be stored and processed securely. By way of example, such applications lie in the fields of health, telephony, pay TV, or banking such as electronic purse applications.

Such cards comprise a plastics card body having an IC or chip device incorporated therein.

In the chip, the integrated circuit forms a complex assembly of logic cells over which a central processor unit (CPU) dispenses and controls information stored in RAM, ROM, or EEPROM type memories by means of a data bus and an address bus.

Conventionally, the logic cells are of the CMOS type. They are constituted by a P-type first MOS transistor and by an N-type second MOS transistor connected in series and controlled by a common logic control signal resulting from the concomitant action of electrical signals present at the inputs of the circuit and of electrical signals generated by programs contained in the ROM or EEPROM memories or by associated electronic circuits. As a function of the logic control signal, charge distribution between valance and conduction bands is altered, thereby giving rise to controlled switching of said transistors.

Nevertheless, some energy sources can also modify this distribution. This applies in particular to electromagnetic radiation, in particular in ranges going from ultraviolet to infrared. As a result, using such radiation to illuminate a zone of the chip, e.g. a set of logic cells, can cause the transistors in said set of cells to switch independently of any electrical control ordered by the logic circuits.

That is why attackers, by taking a chip connected via its Vdd, Vss, Clock, I/O, and Reset pads, and by illuminating an appropriate zone of its circuits with focused electromagnetic radiation in the ultraviolet, visible, or infrared range at a time t chosen by them, have been able to cause the transistors in said zone to switch, thereby altering the normal sequencing of operations programmed in the memories of the chip, and have in particular been able to cause the chip to perform operations that are normally not authorized, thus giving access to secrets without destroying the circuits.

Known means for protecting integrated circuits against the action of electromagnetic radiation have nevertheless been developed. These comprise software means characterized by the fact that the programs in the ROM and EEPROM memories of the chip are numerous and associated with verification means. Nevertheless, those known means do not provide effective protection against "light" attack and they suffer from the drawbacks of requiring a large amount of memory space in the chip and of significantly slowing down the execution of the operations it is required to perform.

From the above, a technical problem which the invention seeks to solve is that of providing a chip for a chip-containing portable article, in particular an article of card format, the chip comprising firstly a silicon substrate layer whose active face has circuits integrated therein defining a central processor unit and memories, and secondly an additional layer of silicon covering at least part of said active face, which chip is not sensitive to the action of electromagnetic radiation in the ultraviolet, visible, and infrared ranges.

According to the invention, a solution to this technical problem consists in that the chip further comprises physical means for providing physical protection against the action of electromagnetic

radiation ~~in the~~ infrared range at a wavelength longer than 1 μm.

Specifically, these physical means for providing protection against the action of electromagnetic radiation are dopants for silicon, or they are formed by surface irregularities or by at least one metal layer.

The invention will be better understood on reading the following non-limiting description given with reference to the accompanying drawings, in which:

- Figure 1 is a perspective view of a card having a chip of the invention;
- Figure 2 is a perspective view of a module including a chip of the invention;
- Figure 3A and 3B are perspective views showing two types of chip of the invention;
- Figures 4A, 4B, and 4C are cross-sections through three variants of a first embodiment of a chip of the invention;
- Figures 5A and 5B are graphs showing the extent to which the means of the invention provide the chip with protection against the action of light;
- Figures 6A, 6B, 6C, and 6D are cross-sections showing four variants of a second embodiment of a chip of the invention; and
- Figures 7A, 7B, 7C, and 7D are cross-sections showing four variants of a third embodiment of a chip of the invention.

The present invention deals by way of example with smart cards, nevertheless, the invention naturally applies in general to any integrated circuit device for incorporation in a portable article, such as a subscriber identity module (SIM) of mini-card format, or an electronic label.

A smart card is a standard portable article operating with and/or without contact and it is defined in particular in ISO standards 7810 and 7816, the content

of which is incorporated in the present description by reference.

As shown in Figure 1, a smart card comprises firstly a plastics card body 2 and secondly an electronic module 3 having contact areas 4 lying flush with the surface of the card body 2.

The card body 2 is made of a plastics material which can be thermoplastic or thermosetting. It is in the form of a flat rectangular parallelepiped having dimensions which are about 85 millimeters (mm) long, 54 mm wide, and 0.76 mm thick.

The electronic module 3 shown in Figure 2 comprises an integrated circuit or chip device 5 fixed via its rear surface 6 to a thickness 7 of epoxy that carries the contact areas 4. Contact pads 8 on the chip 5 are electrically connected to said areas 4 by means of metal wires passing through holes 10 opening out through the thickness 7 of epoxy. The assembly comprising the chip 5 and the wires 9 is embedded in a protective resin 11.

Chips 5 of the invention are in the form of small rectangular parallelepipeds, in practice having a side of about 2 mm and a thickness of a few hundreds of microns (μm), e.g. 200 μm. There are two main types.

In a first type as shown in Figure 3A, the chip 5 has a silicon substrate layer 12. This layer 12 has an active face 13 in which the circuits are integrated and a face opposite from said active face 13, i.e. the rear face 6. The contact pads 8 are generally five in number and they are integrated in the active face 13.

In a second type shown in Figure 3B, the chip 5 has in similar manner a silicon substrate layer 12 whose rear face 8 has been thinned. This silicon substrate layer 12 likewise has an active face 13 which includes the integrated circuits and a face opposite said active face, i.e. the rear face 6. However, the active face 13 is covered in an additional layer 14 of silicon which is sealed to said face 13 via a sealing layer 15. The

additional layer 14 has a top face 18 and a bottom face 19 in contact with the sealing layer. The sealing layer 15 and the additional layer 14 advantageously cover all or at least a major portion of the active face 13 of the chip 5 with the exception of the contact pads 8 which remain accessible through openings 16 or "vias" formed through said layers 14 and 15. In practice, the thicknesses of the various layers are as follows. Thinned substrate layer: about 15 µm; additional layer: about 150 µm; and sealing layer: about 10 µm.

Whatever its type, the chip 3 of the invention has physical means providing physical protection against the action of light, i.e. against the action of electromagnetic radiation in the ultraviolet, visible, and infrared ranges, said ranges being defined as follows by wavelength:

- ultraviolet: 10 nanometers (nm) < λ < 400 nm;
- visible: 400 nm < λ < 700 nm; and
- infrared: 0.7 µm < λ < 0.1 mm.

In a first embodiment of the invention as shown in Figures 4A, 4B, and 4C, these means are silicon dopants 17.

In an intrinsic silicon crystal, all or nearly all of the atoms are silicon atoms. As shown in Figure 5A, an intrinsic silicon crystal at 300 Kelvins (K) is opaque to electromagnetic radiation in most of the visible and ultraviolet spectrum at a wavelength longer than 0.7 µm, having an absorption coefficient greater than 100 cm^{-1}. However, this absorption coefficient falls off very considerably at wavelengths greater than 1 µm, i.e. for the portion of the electromagnetic spectrum that corresponds substantially to the infrared range. Infrared radiation therefore penetrates intrinsic silicon.

As shown in Figure 5B, in the presence of dopants 17 at a concentration of $N_d = 10^{19}$ atoms per cm^3, the light absorption coefficient remains greater than 100 cm^{-1}, not

only at wavelengths shorter than 1 μm, but also at longer wavelengths. It can even be seen that the absorption coefficient increases at wavelengths rising from 1 μm to 10 μm.

Thus, the dopants conventionally used for changing the semiconductive properties of silicon are capable of changing the absorption properties of an intrinsic crystal of silicon so that its absorption coefficient increases significantly at wavelengths longer than 1 μm, i.e. in particular, at wavelengths in the infrared range.

In the invention, the dopants 17 are atoms whose chemical nature is different from that of silicon such that the presence thereof gives rise to defects in its crystal lattice. They can be atoms of phosphorus or of boron, for example. The number of dopant atoms present in the silicon lies in the range 10^{17} to 10^{20} atoms per cm^3, and is preferably about 10^{19} atoms per cm^3. Light absorption at given wavelength and thickness increases with increasing concentration of dopant.

The dopants 17 can be incorporated in the crystal lattice while the silicon crystal is being grown, or else they can be the subject of high temperature diffusion under an inert atmosphere, or they can be the subject of ion implantation.

The dopants 17 can be present in the silicon substrate layer 12 of a chip 5 of the first type or of a chip 5 of the second type. They can also be incorporated in the additional layer 14 of a chip 5 of the second type.

In the variant of Figure 4A which shows a chip 5 of the second type, the dopants 17 are present in the additional layer 14 of the chip 5. They are uniformly distributed throughout this layer 14. Nevertheless, they could be concentrated solely in a fraction of the thickness of said layer 14, in particular in the portion of said layer that is close to its top face 18.

In the variant of Figure 4B which shows a chip 5 of the first type, the dopants 17 are present in the substrate layer 12 of the chip 5. These dopants are concentrated in the rear portion of said layer 12. Thus, the effects of the dopants on electrical conduction do not interfere with proper operation of the integrated circuits on the active face 13 of the chip 5.

In the variant of Figure 4C which shows a chip 5 of the second type, the dopants 17 are present both in the substrate layer 12 of the chip and in its additional layer 14.

Sub A2

In a second embodiment of the invention as shown in Figures 6A, 6B, and 6C the means providing physical protection against the action of light are formed by surface irregularities 20 visible on a face of a layer of silicon. These surface irregularities can be visible on the rear face of the silicon substrate or on one or two of the top and bottom faces of the additional layer 14 for chips 5 of the second type.

By way of example, these surface irregularities 20 are constituted by recesses and projections formed over the entire surface in question of the substrate or additional layer. The height of these recesses and projections is of the order of a few microns.

In practice, the irregularities 20 are formed by etching the silicon, e.g. by means of a dry technique such as mechanical abrasion, or a wet technique such as potassium hydroxide (KOH) machining.

Focused incident electromagnetic radiation, and in particular such electromagnetic radiation having a wavelength longer than 1 μm, in particular infrared radiation, is reflected in part by the irregular walls of the silicon and is subject in part to refraction. By being reflected, attenuated, and diffused in this way, the radiation no longer reaches the intended targets of the attacker and the attacker can no longer predict which

targets will finally be reached. This makes attack impossible.

In the variant of Figure 6A which shows a chip 5 of the second type, the irregularities 20 are formed on the face of the additional layer 14 which comes into contact with the sealing layer 15.

In the variant of Figure 6B which shows a chip 5 of the first type, the irregularities 20 are formed in the rear face of the silicon substrate layer.

Sub A13

In the variant of Figure 6C which shows a chip 5 of the second type, the irregularities 20 are formed in the face 18 of the additional layer.

In the variant of Figure 6D which shows a chip 5 of the second type, the irregularities 20 are formed in the top face 18 of the additional layer 14, in its bottom face 19, and in the rear face 6 of the chip 3.

In a third embodiment of the invention shown in Figures 7A, 7B, and 7C, the physical protection means are formed by a metal layer 21 assembled on at least one of the faces of the substrate or additional layers 12 or 14 of silicon and having a thickness of more than 50 Ångstroms (Å), e.g. about 100 Å.

By way of example, this can be a layer of aluminum, of palladium, or a layer made up of a superposition of metal sub-layers, e.g. of nickel, of chromium, and of gold.

A face can be metallized by vacuum deposition.

The layer of metal reflects or absorbs all of the incident light that is intended to illuminate the circuits. It is no longer possible to use an optical microscope to inspect the active surface of the integrated circuit nor is it possible to observe it using infrared techniques.

In the variant of Figure 7A which shows a chip of the second type, the metal layer 21 is placed between the additional layer 14 and the sealing layer 15.

In the variant of Figure 7B which shows a chip of the first type, the metal layer 21 is placed on the rear face of the substrate layer 12.

In the variant of Figure 7C which shows a chip 3 of the second type, the metal layer 21 is placed on the top face 18 of the additional layer 14.

In the variant of Figure 7D which shows a chip 3 of the second type, a first metal layer is placed between the additional layer 14 and the sealing layer 15, and a second metal layer is placed on the rear face of the substrate layer 12.

Naturally, the invention is not limited to the above-described variants. In addition, it is possible to use different protection means in the same chip 5.

It will be observed that installing an additional layer on the active face of a chip of the first type and/or installing the above-mentioned means for protecting the circuits against the action of light can take place in steps that are subsequent to the conventional steps for producing integrated circuits. As a result, conventional chip manufacturing lines can be conserved. Furthermore, a chip of the invention, whether of the first type or of the second type, has substantially the same dimensions as conventional chips in the state of the art. As a result lines for manufacturing modules can be conserved to operate with chips of the invention.

It will also be observed that the means providing physical protection against the action of light can cover all of the integrated circuits or only some of them. When only certain portions of said integrated circuits are covered, those portions are advantageously key portions, i.e. portions which are sensitive to attack by light and in which a disturbance produced by such light could be harmful to the integrity of the chip and the secrets it contains. In particular, such key portions can be constituted by the voltage multiplier used for

programming the EEPROM memory cells, the amplifiers for reading the content of the memories, and some of the registers of the volatile memory (RAM) or of the central processor unit (CPU).